

# (12) UK Patent Application (19) GB (11) 2 004 673 A

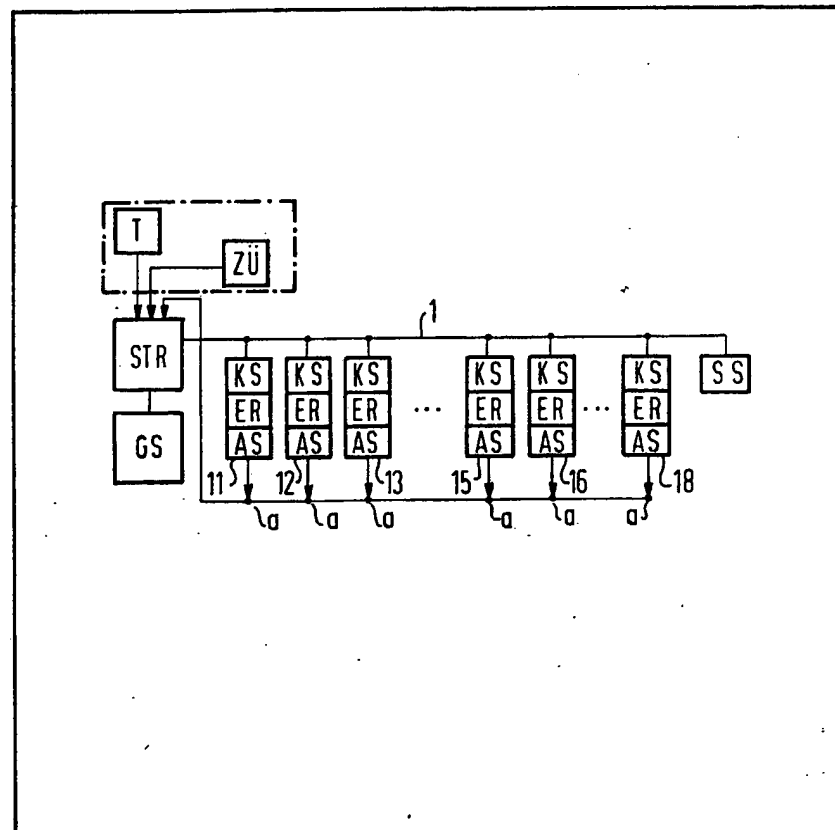
- (21) Application No: 7836732  
(22) Date of filing:  
13 SEP 1978  
(23) Claims filed:  
13 SEP 1978  
(30) Priority data:  
(31) 2741379  
(32) 14 SEP 1977  
(33) FED. REP. OF  
GERMANY (DE)  
(43) Application published:  
4 APR 1979  
(51) INT. CL.: G06F 11/00  
(52) Domestic classification:  
G4A 12N 12P 12T ES  
(56) Documents cited:  
GB 1412246  
GB 1411182  
GB 1243464  
GB 1168414  
DE 2546202A  
(58) Field of search:  
G4A  
H4K  
(71) Applicants:  
SIEMENS AKTIEN-  
GESELLSCHAFT,  
BERLIN AND  
MUNICH, FEDERAL  
REPUBLIC OF  
GERMANY  
(72) Inventor:  
RUDOLF KOBER  
(74) Agents:  
G. F. REDFERN & CO.

## (54) COMPUTER SYSTEM

(57) A computer system has two or more computer modules (11 to 15) coordinated by a control computer (STR) via a system bus (1) and each comprising an individual computer and local storage (ER, KS), and a safeguarding store (SS) in which during periodic monitoring phases, the intermediate results of the modules are stored. When a fault situation is recognised during a

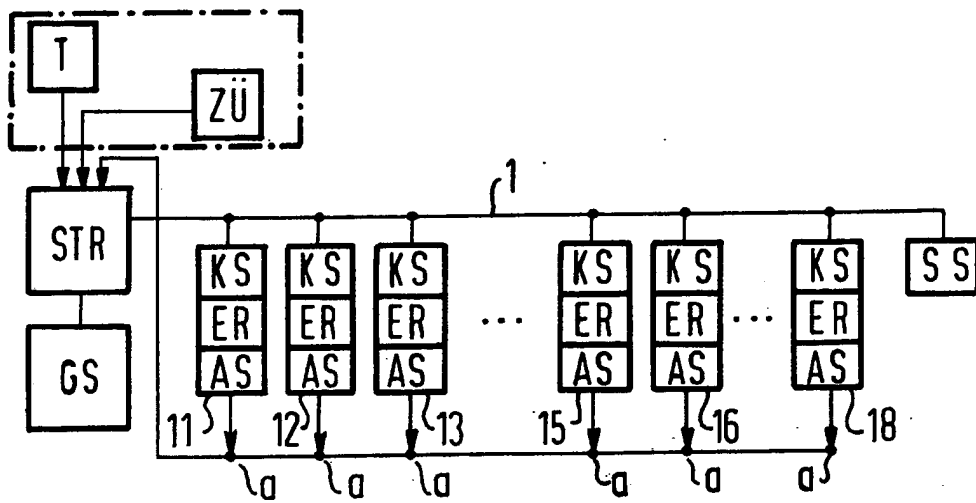
monitoring phase, a defective module can be replaced and, since a set of (correct) intermediate results is stored in the safeguarding store the system can then use these results to return to the corresponding point in execution and resume processing from that point without undue delay.

The arrangement is used in real time applications such as process control and monitoring equipment where high reliability and minimum time loss in the event of a fault are required.



GB 2 004 673 A

2004673



## SPECIFICATION

## COMPUTER SYSTEM

The present invention relates to computer systems and methods of operating such systems. It is particularly, though not exclusively, concerned with systems wherein two or more computer modules, each consisting of an individual computer, a coupling store and a working store, can be coupled to a system bus consisting of a control- and address-bus and a data bus, wherein access can be gained to a coupling store either from the system bus or from the individual computer by switching over, and wherein only the individual computer has access to its working store and wherein the system bus can be coupled to a control computer.

A computer system of the type described in the introduction is described in German Offenlegungsschrift 2 546 202. This computer system operates in a three-phase operation. The first phase consists of a control phase during which only the control computer is operative: it executes its programme and informs the individual computers of the function which they must carry out during the following phase. The second phase consists of an autonomous phase during which the individual computers carry out their assigned functions simultaneously and independently of one another without being connected to the control computer or its store, and then report the execution of their function by transmitting a "STOP" signal to the control computer. The third phase consists of a data exchange phase which starts when the control computer has received a "STOP" signal from all of the individual computers or from a selection of individual computers established by the circuit, and during which, under the control of the control computer, data exchange is carried out between the stores of the individual computers and possibly of the control computer.

For certain fields of use of data processing systems, for example in process control monitoring, for example of nuclear power stations and in navigation systems for missiles, computer systems having a particularly high degree of reliability are required.

The reliability of data processing systems can be increased by redundancy in construction, e.g. by a multiple provision of critical components: for example by a central unit with a working store, in which, in the case of differing results, the result emitted by the majority of components is used, or else by a redundancy in organisation for example by means of redundant, fault-correcting codes. A fundamental requirement of computer organisation consists in being able to continue computation without or with only a low time loss on the occurrence of faults. It is not sufficient to isolate and replace faulty components and then to recommence the function being processed from the start. Even if this were possible, the resultant time loss would generally be incompatible with

the requirements of real time problems.

65 The aim of the present invention is to provide a computer system which facilitates real time operation in the event of breakdown of individual components.

In one aspect the invention provides a computer system comprising a plurality of computer modules each having an individual computer and local store facilities, a programme store, a control computer which coordinates operation of one or some of the modules for execution of the programme, and a safeguarding store, the system being so arranged that during execution of a programme the system periodically assumes a monitoring phase in which, in the absence of faulty operation the intermediate results produced by the computer modules are stored in the safeguarding store, and upon recognition of a fault the module(s) affected are replaced by others and the intermediate results last stored in the safeguarding store are transferred therefrom to the computer modules whereby the system returns to the situation obtaining at the last monitoring phase in which no faults were recognised and resumes processing from that point.

90 In another aspect the invention provides a method for the operation of a computer system comprising a plurality of computer modules each having an individual computer and local store facilities, a programme store, a control computer which coordinates operation of one or some of the modules for execution of the programme, and a safeguarding store, in which: the control computer, the further store and one or some of the modules are used to process the user programme; a monitoring phase is periodically inserted in which all the individual computers are checked for functioning capacity whereby defective modules are identified; in the event that no defective modules are recognised the intermediate results calculated at that time are stored in the safeguarding store and the further processing of the user programme is continued; in the event that one or more than one defective module is recognised the one or each of these is replaced by one of the remaining modules not already in use for processing the user programme, for which purpose the individual function of the module to be replaced is loaded from the further store which stores the entire user programme into each replacing module, and that then further processing is continued with the last safeguarded intermediate results from the safeguarding store.

115 Preferably the computer system processes the user programmer in a three-phase cycle.

120 Preferably the computer system is operated in such manner that after as few as possible phase cycles a monitoring phase is additionally inserted between autonomous phase and the next data exchange phase.

125 For the triggering of the monitoring phases the computer system may advantageously be equipped with a pulse generator which is coupled to the

control computer and which triggers the monitoring phases in time with the pulse period thereof.

In order to exchange a defective module for an intact module, it is expedient for each module to be provided with a fixed module number and a module number which can be modified by the control computer for characterisation purposes. The exchange process is then expediently carried out in that the modifiable module numbers of the defective modules are exchange with those of intact modules, their fixed module numbers being used for addressing purposes.

Advantageously the computer system may be equipped with a time monitoring device which is coupled to the computer system and which indicates an impermissibly long autonomous phase and immediately introduces an additional monitoring phase.

The computer system can advantageously be designed in such manner that each module possesses a parity production and checking unit which constantly monitors the module and on the recognition of a defect reports this defect to the control computer by means of a parity fault message and thus immediately triggers a monitoring phase.

An exemplary embodiment of the invention will now be described with reference to the accompanying drawing, which is a block diagram of a computer system.

The computer system comprises computer modules 11, 12, 13, ... 15, 16 ... 18 coupled to the system control, address and data bus 1. Each module comprises a coupling store KS, an individual computer ER and a working store AS. In each module, only the individual computer has access to its own working store, whereas access can be obtained to the coupling store selectively from both the individual computer and from the system bus. For purposes of fault recognition each module is equipped with a parity generating and checking unit and possesses its own output  $\alpha$  for parity fault messages. Each module is assigned a fixed module number and a module number which can be modified by the control computer. Furthermore a control computer STR is provided which can be coupled to the system bus 1, has access to a further working store GS and has access via this system bus to a safeguarding store SS. The further store preferably consists of a high speed large capacity store, for example a disc store. All the individual computers are preferably micro-processors. The safeguarding store is preferably identical in construction to the coupling store of a module. Also provided are a pulse generator T and a time monitoring device ZÜ which are both coupled to the control computer. The pulse period of the pulse generator regularly triggers monitoring phases. All the outputs  $\alpha$  of the computer modules are similarly connected to the control computer.

In the following the cooperation of all the described components will be explained. It has been assumed that the modules 11 to 15 are used

to process the user programme whereas the modules 16 to 18 are redundant modules. The computer system which processes the user programme consists of the modules 11 to 15, the control computer and the further store and can simultaneously process as many sub-functions of the user programmer as computer modules 11 to 15 are provided. The computer system operates in the three-phase cycle described in the

introduction, i.e. control phase; autonomous phase; data transfer. The computer state following each three-phase cycle is defined by the individual functions stored in the modules and by the exchanged results which are primarily intermediate results.

Whereas the individual functions are fixed and can be called up for example from the further store, the intermediate results must be safeguarded. This, together with a check on the computer, is carried out in additionally interposed monitoring phases.

The duration between two monitoring phases is determined by the period of the pulse generator T. The pulse generator transmits an interrupt request to the control computer which inserts a monitoring phase before the next data exchange phase.

The control computer starts test programmes which are provided in all the modules and which carry out a function check of the modules. Here it is necessary to use test programmes which, in the case of fault-free modules, do not permanently alter the store contents. Fault messages are stored in the coupling store KS. The control computer now checks whether fault messages have been received from modules entrusted with the processing of a sub-function. If none has been received the safeguarding store is coupled to the system bus for the following data exchange phase in order to receive the intermediate results simultaneously with the coupling stores of the modules entrusted with the sub-functions. The further processing of the user programme is then continued without modification. If, however, faults occur the defective modules are replaced by intact, previously unused modules.

This is carried out in the following steps: the module numbers, modifiable by the control computer, of the free and defective modules are exchange, addressing during this procedure being effected using the fixed module numbers. Then the missing individual functions are reloaded from the further store which stores the user programme in full. For the duration of the next data exchange phase the safeguarding store is coupled to the system bus. In contrast to a fault-free situation in which the intermediate results have been written into the safeguarding store, it now forms the source of safeguarded results. These are read out from the safeguarding store and transferred into the coupling stores.

This fulfils the conditions for the restarting of the system. The starting point is the control phase which follows the last phase cycle with a fault-free monitoring phase.

Apart from the pulse generator T, monitoring phases can also be triggered by the time monitoring device ZU which indicates an impermissibly long autonomous phase or by a parity fault message from one of the modules which appears at the output  $\alpha$ . In these situations the modules are checked immediately without waiting for the conclusion of the autonomous phase.

## 10 CLAIMS

1. A computer system comprising a plurality of computer modules each having an individual computer and local store facilities, a programme store, a control computer which coordinates operation of one or some of the modules for execution of the programme, and a safeguarding store, the system being so arranged that during execution of a programme the system periodically assumes a monitoring phase in which, in the absence of faulty operation the intermediate results produced by the computer modules are stored in the safeguarding store, and upon recognition of a fault the module(s) affected are replaced by others and the intermediate results last stored in the safeguarding store are transferred therefrom to the computer modules whereby the system returns to the situation obtaining at the last monitoring phase in which no faults were recognised and resumes processing from that point.

2. A computer system as claimed in claim 1, comprising, for the triggering of monitoring phases, a pulse generator which is coupled to the control computer and triggers the monitoring phases in time with the pulse period of the pulse generator.

3. A computer system as claimed in claim 1 or 2, and further including a time monitoring unit which is connected to the control computer, and is, in use, responsive to the occurrence of an impermissibly long autonomous phase to immediately initiate an additional monitoring phase.

4. A computer system as claimed in claim 1, 2 or 3, in which each module possesses a parity production and checking unit which constantly monitors the module and on the recognition of a defect reports this defect to the control computer by a parity fault message and immediately triggers a monitoring phase.

5. A method for the operation of a computer system comprising a plurality of computer modules each having an individual computer and local store facilities, a programme store, a control computer which coordinates operation of one or some of the modules for execution of the programme, and a safeguarding store, in which: the control computer, the further store and one or some of the modules are used to process the user programme; a monitoring phase is periodically inserted in which all the individual computers are

checked for functioning capacity whereby defective modules are identified; in the event that no defective modules are recognised the intermediate results calculated at that time are stored in the safeguarding store and the further processing of the user programme is continued; in the event that one or more than one defective module is recognised the or each of these is replaced by one of the remaining modules not already in use for processing the user programme, for which purpose the individual function of the module to be replaced is loaded from the further store which stores the entire user programme into each replacing module, and that then further processing is continued with the last safeguarded intermediate results from the safeguarding store.

6. A method as claimed in claim 5, in which the check on the functioning capacity of the individual computers is carried out by means of test programmes stored in the local stores of the modules.

7. A method as claimed in claim 5 or 6, in which the computer system processes the user programme in a three-phase cycle.

8. A method as claimed in claim 7, in which after as few as possible phase cycles a monitoring phase is additionally interposed between autonomous phase and the next data exchange phase.

9. A method as claimed in any one of claims 5 to 8, in which for characterisation each module is assigned a fixed module number and a module number which can be modified from the control computer.

10. A method as claimed in claim 9, in which the exchange process by means of which a defective module is replaced by another module is carried out in such manner that the modifiable module numbers of the defective modules are exchanged with those of intact modules, their fixed module numbers being used for addressing purposes.

11. A computer system substantially as herein described with reference to the accompanying drawing.

12. A method of operating a computer system as claimed in claim 1, substantially as herein described.

13. A computer system comprising: at least two or more computer modules each consisting of an individual computer, a coupling store and a working store; a system bus consisting of a control- and address-bus and a data bus, the coupling store of each module being accessible both from the system bus and from the individual computer of that module and the working store of each module being accessible from the individual computer of that module; a control computer having access to the system bus; a safeguarding store to which the control computer has access via the system bus; and a further store to which the control computer has access are provided.